Conference proceedings | © 2023

Proceedings of Third International Conference on Computing, Communications, and Cyber-Security

IC4S 2021

Editors: Pradeep Kumar Singh, Sławomir T. Wierzchoń, Sudeep Tanwar, Joel J. P. C. Rodrigues, Maria Ganzha

Presents recent research in the field of computing and communication

Discusses the outcomes of IC4S 2021, held in Ghaziabad, India

Serves as a reference guide for researchers and practitioners in academia and industry

Part of the book series: Lecture Notes in Networks and Systems (LNNS, volume 421)

Sections

Table of contents (70 papers)

Search within book

← Previous Page 2 of 4 Next →

Advanced Computing Technologies

Data Analytics and Intelligent Learning

← Previous Page 2 of 4 Next →

Back to top ↑

About this book

This book features selected research papers presented at the Third International Conference on Computing, Communications, and Cyber-Security (IC4S 2021), organized in Krishna Engineering College (KEC), Ghaziabad, India, along with Academic Associates; Southern Federal University, Russia; IAC Educational, India; and ITS Mohan Nagar, Ghaziabad, India, during October 30–31, 2021. It includes innovative work from researchers, leading innovators, and professionals in the area of communication and network technologies, advanced computing technologies, data analytics and intelligent learning,

Proceedings of Third International Conference on Computing, Communications, and Cyber-Security pp 311–323

Execution Survey and State of the Art of Different ML-Based Ensemble Classifiers Approach Contextual Analysis of Spam Remark Location

Biswajit Mondal & Subir Gupta

Conference paper | First Online: 03 July 2022

Part of the Lecture Notes in Networks and Systems book series (LNNS,volume 421)

Abstract

The digital podium is proving as an increasingly important area for the contemporary development of civilization. However, it additionally engenders a rudimentary conundrum. Spamming is one of the most solemn quandaries that puts state-of-the-art security to the test. Spam wires, which send offensive messages to an immensely voluminous number of recipients, conventionally have become an apperceived security peril. There are various ways spam security issues can be addressed, including utilizing a machine learning (ML) complement system. Ensemble classifier is one of

the most commonly used ML approximations. Ensemble methods use different models to amend execution. In various examination fields, like computational erudition, stats, and machine learning uses ensemble classifiers. This paper surveys traditional and verbally express-of-the-art ensemble approaches, accommodating a comprehensive overview for both practitioners and newcomers. In customary outfit strategies like Ada boost, Bagging classifier, extra trees sorts the ensemble techniques; gradient boost; logit boost; random forest; real Ada boost. This investigation is fixated on the ensemble frameworks to slant toward the spam (channel spam or ham remarks) security issue. Remark datasets are utilized for a fascinating judgment of over 41k comments and not for spam. We can split the experimental dataset into two parts. The first uses 30k for training, and the second utilizes the remaining 10k for testing. End-of-heuristics evaluation utilizing accuracy, precision, recall, *f*1 score, AUC score, model preparation time, and mean squared error reveals that Extra Trees outperforms numerous models in various exhibit metrics.

Keywords

Ada boost **Bagging classifier** **Extra trees**

Gradient boost **Logit boost**

Random forest **Real Ada boost**

References

1. Mewada, A., & Dewang, R. K. (2021). Research on false review detection methods: A state-of-the-art review. *Journal of King Saud University and Computer and Information Sciences*, (xxxx). https://doi.org/10.1016/j.jksuci.2021.07.021

2. Petschke, D., & Staab, T. E. M. (2019). A supervised machine learning approach using naive Gaussian Bayes classification for shape-sensitive detector pulse discrimination in positron annihilation lifetime spectroscopy (PALS). *Nuclear Instruments and Methods in Physics Research, Section A: Accelerators Spectrometers, Detectots and Associated*

Equipment, 947, 162742. https://doi.org/10.1016/j.nima.2019.162742

3. Ning, B., Junwei, W., & Feng, H. (2019). Spam message classification based on the naïve Bayes classification algorithm. *IAENG International Journal of Computer Science, 46*(1).

4. Samuel, A. L. (1959). Eight-move opening utilizing generalization learning. (See Appendix B, Game G-43.1 Some Studies in Machine Learning Using the Game of Checkers) *IBM Journal*, 210–229.

5. Gupta, S., Sarkar, J., Kundu, M., Bandyopadhyay, N. R., & Ganguly, S. (2020). Automatic recognition of SEM microstructure and phases of steel using LBP and random decision forest operator. *Measurement, 151*(xxxx), 107224. https://doi.org/10.1016/j.measurement.2019.107224

6. Gupta, S. et al. (2020). Modelling the steel microstructure knowledge for in-silico recognition of phases using machine learning. *Materials Chemistry and Physics, 252*, 123286. https://doi.org/10.1016/j.matchemphys.2020.123286

7. Mondal, B. (2020). Artificial intelligence: State of the art. *Intelligent Systems Reference Library, 172*,

389–425.

8. Ligthart, A., Catal, C., & Tekinerdogan, B. (2020). Analyzing the effectiveness of semi-supervised learning approaches for opinion spam classification. *Applied Soft Computing, 101*, 107023. https://doi.org/10.1016/j.asoc.2020.107023

9. Padmanabha Reddy, Y. C. A., Viswanath, P., & Eswara Reddy, B. (2018). Semi-supervised learning: a brief review. *International Journal of Engineering and Technology, 7*(1.8), 81. https://doi.org/10.14419/ijet.v7i1.8.9977

10. Panahi, R., Ebrahimie, E., Niazi, A., & Afsharifar, A.(2021). Integration of meta-analysis and supervised machine learning for pattern recognition in breast cancer using epigenetic data. *Informatics in Medicine Unlocked, 24*, 100629, 2021. https://doi.org/10.1016/j.imu.2021.100629

11. Wang, Y., et al. (2020). Unsupervised machine learning for the discovery of latent disease clusters and patient subgroups using electronic health records. *Journal of Biomedical Informatics, 102*, 103364. https://doi.org/10.1016/j.jbi.2019.103364

12. Reisach, U. (2021). The responsibility of social media in times of societal and political manipulation. *European Journal of Operational Research, 291*(3), 906–917. https://doi.org/10.1016/j.ejor.2020.09.020

13. Engström, E., & Strimling, P. (2020). Deep learning diffusion by infusion into preexisting technologies—Implications for users and society at large. *Technology in Society, 63*, 101396. https://doi.org/10.1016/j.techsoc.2020.101396

14. Gao, H., Cheng, S., & Zhang, W. (2021) GDroid: Android malware detection and classification with graph convolutional network. *Computers & Security, 106*. https://doi.org/10.1016/j.cose.2021.102264

15. Sharmila, V., Rejin Paul, N. R., Ezhumalai, P., Reetha, S., & Naresh Kumar, S. (2020). IOT enabled smart assistance system using face detection and recognition for visually challenged people. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2020.10.198

16. Piryonesi, S. M., & El-Diraby, T. E. (2020). Role of data analytics in infrastructure asset management: Overcoming data size and quality problems. *Journal of Transportation*

Engineering: Part B Pavements, 146(2), 04020022. https://doi.org/10.1061/jpeodx.0000175

17. Yang, S., Wu, J., Du, Y., He, Y., & Chen, X. (2017). Ensemble learning for short-term traffic prediction based on gradient boosting machine. *Journal of Sensors*. https://doi.org/10.1155/2017/7074143

18. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things, 7*, 100059. https://doi.org/10.1016/j.iot.2019.100059

19. El-Dairi, M., & House, R. J. (2019). Optic nerve hypoplasia. In *Handbook of Pediatric Retinal OCT and the Eye-Brain Connection* (pp. 285–287). https://doi.org/10.1016/B978-0-323-60984-5.00062-7

20. Benussi, A., et al. (2021). Classification accuracy of TMS for the diagnosis of mild cognitive impairment. *Brain Stimulation, 14*(2), 241–249. https://doi.org/10.1016/j.brs.2021.01.004

21. Louzada, F., & Ara, A. (2012). Bagging k-dependence probabilistic networks: An alternative powerful fraud detection tool.

Expert Systems with Applications, 39(14), 11583–11592. https://doi.org/10.1016/j.eswa.2012.04.024

22. Moral-García, S., Mantas, C. J., Castellano, J. G., Benítez, M. D., & Abellán,J. (2020). Bagging of credal decision trees for imprecise classification. *Expert Systems with Applications, 141*. https://doi.org/10.1016/j.eswa.2019.112944

23. Besharati, E., Naderan, M., & Namjoo, E. (2018). LR-HIDS: Logistic regression host-based intrusion detection system for cloud environments. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-018-1093-8

24. Padmaja, B., Prasad, V. V. R., & Sunitha, K. V. N. (2020). A novel random split point procedure using extremely randomized (Extra) trees ensemble method for human activity recognition. *EAI Endorsed Transactions on Pervasive Health and Technology, 6*(22), 1–10. https://doi.org/10.4108/eai.28-5-2020.164824

25. Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things*, *14*,

100393. https://doi.org/10.1016/j.iot.2021.100393

26. Mateen, M., Wen, J., Nasrullah, Song, S., & Huang, Z. (2019). Fundus image classification using VGG-19 architecture with PCA and SVD. *Symmetry (Basel), 11*(1). https://doi.org/10.3390/sym11010001

27. Thakur, S., Chakraborty, A., De, R., Kumar, N., & Sarkar, R. (2021). Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model. *Computers & Electrical Engineering, 91*. https://doi.org/10.1016/j.compeleceng.2021.107044

28. Sun, X. F., & Lin, X. G. (2017). Random-forest-ensemble-based classification of high-resolution remote sensing images and nDSM over urban areas. In *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences—ISPRS Archives, 42*(2W7), 887–892. https://doi.org/10.5194/isprs-archives-XLII-2-W7-887-2017

29. Wazarkar, S., & Keshavamurthy, B. N. (2018). A survey on image data analysis through clustering techniques for real world applications. *Journal of Visual Communication*

and Image Representation, 55, 596–626. https://doi.org/10.1016/j.jvcir.2018.07.009

30. Maeder, M., McCann, N., Clifford, S., & Puxty, G. (2020). *Model-based data fitting* (2nd Ed.., Vol. 3). Elsevier.

31. Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications, 186*. https://doi.org/10.1016/j.eswa.2021.115742

Acknowledgements

We are acknowledging Priyanka Dhara, Shubham Bhattacharjee, and Sohom Bhattacharya for technical help.

Author information

Authors and Affiliations

Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal, 713206, India

Biswajit Mondal & Subir Gupta

Corresponding author

Correspondence to Subir Gupta .

Editor information

Editors and Affiliations

Department of Computer Science, KIET Group of Institutions, Ghaziabad, Delhi, India
Pradeep Kumar Singh

Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland
Sławomir T. Wierzchoń

Department of Computer Science and Engineering, Nirma University, Ahmedabad, India
Sudeep Tanwar

Federal University of Piauí, Teresina, Brazil
Joel J. P. C. Rodrigues

Faculty of Mathematics and Informatics, Warsaw University of Technology, Warsaw, Poland
Maria Ganzha

Rights and permissions

Copyright information

About this paper

Cite this paper

Mondal, B., Gupta, S. (2023). Execution Survey and State of the Art of Different ML-Based Ensemble Classifiers Approach Contextual Analysis of Spam Remark Location. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues,

J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_24

DOI
https://doi.org/10.1007/978-981-19-1142-2_24

Published	Publisher Name	Print ISBN
03 July 2022	Springer, Singapore	978-981-19-1141-5

Online ISBN	eBook Packages
978-981-19-1142-2	Engineering Engineering (R0)